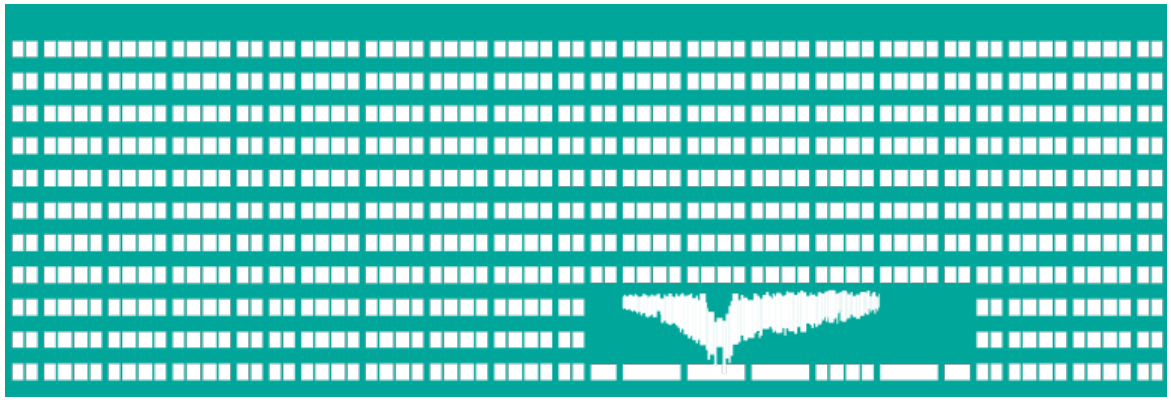
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

Access Control Lists (ACL)



Počítačové sítě
12. cvičení

ACL

- Pravidla pro filtrování paketů (bezestavová)
  - Na základě hlaviček (2.,) 3. a 4. vrstvy
  - Průchod pravidly od 1. k poslednímu
  - Při nalezení odpovídajícího pravidla se další neaplikují
- Výběr rozhraní, na němž bude ACL použito
  - Vstupní rozhraní – nemusí se směrovat zahozené pakety
  - Výstupní rozhraní – jednotné zpracování bez ohledu na původ paketů
- Závěrečné pravidlo
  - Zahoď vše – implicitní, co není povoleno je zakázáno
  - Propusť vše – lze ručně nastavit, atypické
- **Vždy je potřeba povolit i zpětný směr** (SRC↔DST)!

Konstrukce ACL

- Při konstrukci ACL musíme zodpovědět tyto otázky:
  - Filtrovat na vstupu nebo výstupu ze směrovače?
  - Jaké rozhraní směrovače je nejvýhodnější?
  - Jaké protokoly budou povoleny, odkud a kam, jaké jsou jejich porty?
  - Je lepší něco zakázat a zbytek povolit, nebo naopak?

ACL – příklad 1

- Zakažte veškerý provoz, který nesměřuje na proxy server poskytovatele 40.0.0.1

ACL – příklad 1

- Zakažte veškerý provoz, který nesměřuje na proxy server poskytovatele 40.0.0.1

Odchozí směr

Pořadí položky	Povolit / zakázat	Protokol	Zdrojová IP	Zdrojový port	Cílová IP	Cílový port
1	povolit	IP	*		40.0.0.1	
2	zakázat	IP	*		*	

Příchozí směr

Pořadí položky	Povolit / zakázat	Protokol	Zdrojová IP	Zdrojový port	Cílová IP	Cílový port
1	povolit	IP	40.0.0.1		*	
2	zakázat	IP	*		*	

ACL – příklad 2

- Povolte do Internetu protokoly DNS a HTTP(S)

ACL – příklad 2

- Povolte do Internetu protokoly DNS a HTTP(S)

Odchozí směr

Pořadí položky	Povolit / zakázat	Protokol	Zdrojová IP	Zdrojový port	Cílová IP	Cílový port
1	povolit	UDP	*	*	*	53
2	povolit	TCP	*	*	*	53
3	povolit	TCP	*	*	*	80
4	povolit	TCP	*	*	*	443
5	zakázat	IP	*		*	

Příchozí směr

Pořadí položky	Povolit / zakázat	Protokol	Zdrojová IP	Zdrojový port	Cílová IP	Cílový port
1	povolit	UDP	*	53	*	*
2	povolit	TCP	*	53	*	*
3	povolit	TCP	*	80	*	*
4	povolit	TCP	*	443	*	*
5	zakázat	IP	*		*	

Definice položek CISCO ACL

- **access-list** *<č. ACL>* {**permit**|**deny**} *<protokol> <zdrojová_IP> <wildcard_maska>* [*<zdrojový_port>*] *<cílová_IP> <wildcard_maska>* [*<cílový_port>*] [*parametry závislé na protokolu*]
  - Wildcard maska říká, které bity adresy ignorovat a které ne
    - 0=porovnat, 1=ignorovat
    - „Obrácená subnet maska“
  - Port u TCP, UDP: {**eq**|**gt**|**lt**} <č. portu>
  - Parametry závislé na protokolu
    - Typy ICMP zpráv (**echo**, **echo-reply**, …)
    - Zda již musí být TCP spojení navázáno (**established**)
  - …

Syntaktické zkratky

- **any**
  - libovolná IP adresa + wildcard maska **255.255.255.255**
  - *
- **host X.X.X.X**
  - IP adresa X.X.X.X + wildcard maska **0.0.0.0**

- Příklad:
  - **`permit tcp host 158.196.100.100 any eq 80`**

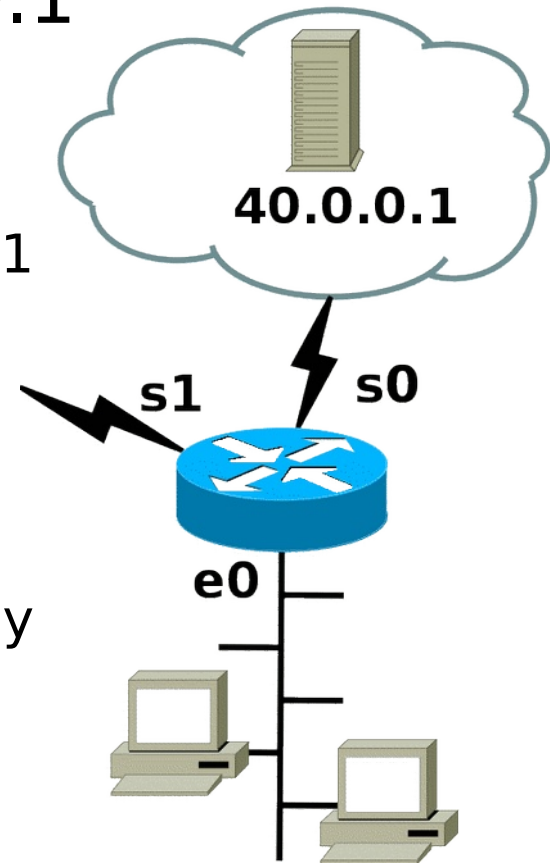
Přiřazení ACL na rozhraní

- **interface** *<rozhraní>*
  ip access-group *<č. acl>* {**in**|**out**}

- Na určité rozhraní se přiřadí ACL identifikovaný číslem
  - **in** – filtruje provoz směrem do rozhraní (vstupující do směrovače)
  - **out** – filtruje provoz směrem z rozhraní (vystupující ze směrovače)

ACL – příklad 1

- Zakažte veškerý provoz, který nesměřuje na proxy server poskytovatele 40.0.0.1
  - Odchozí směr
    - access-list 101 permit ip any host 40.0.0.1
    - **interface e0**
      - **ip access-group 101 in**
  - Příchozí směr
    - access-list 102 permit ip host 40.0.0.1 any
    - **interface e0**
      - **ip access-group 102 out**



ACL – příklad 2

- Povolte do Internetu protokoly DNS a HTTP(S)
- Odchozí směr
  - `access-list 103 permit udp any any eq 53`
  - `access-list 103 permit tcp any any eq 53`
  - `access-list 103 permit tcp any any eq 80`
  - `access-list 103 permit tcp any any eq 443`
- Příchozí směr
  - `access-list 104 permit udp any eq 53  any`
  - `access-list 104 permit tcp any eq 53  any established`
  - `access-list 104 permit tcp any eq 80  any established`
  - `access-list 104 permit tcp any eq 443 any established`

ACL – příklad 3

- Zakažte pro síť 10.0.20.0/24 ICMP provoz s výjimkou použití příkazu ping do vnější sítě

ACL – příklad 3

- Zakažte pro síť 10.0.20.0/24 ICMP provoz s výjimkou použití příkazu ping do vnější sítě
- Odchozí směr
  - `access-list 105 permit icmp 10.0.20.0 **0.0.0.255** any **echo**`
  - `access-list 105 deny icmp 10.0.20.0 **0.0.0.255** any`
  - `access-list 105 permit ip any any`
- Příchozí směr
  - `access-list 106 permit icmp any 10.0.20.0 **0.0.0.255 echo-reply**`
  - `access-list 106 deny icmp any 10.0.20.0 **0.0.0.255**`
  - `access-list 106 permit ip any any`

ACL – příklad 4

- Povolte přístup z vnějšku na POP3 servery v síti 100.10.20.40/30 a SMTP server 100.10.20.45

ACL – příklad 4

- Povolte přístup z vnějšku na POP3 servery v síti 100.10.20.40/30 a SMTP server 100.10.20.45
- Odchozí směr
  - access-list 107 permit tcp 100.10.20.40 **0.0.0.3** eq 110 any **established**
  - access-list 107 permit tcp host 100.10.20.45 eq 25 any **established**
  - access-list 107 permit tcp host 100.10.20.45 any eq 25
  - (následovat by měla pravidla zpřístupňující DNS serverům)
- Příchozí směr
  - access-list 108 permit tcp any 100.10.20.40 **0.0.0.3** eq 110
  - access-list 108 permit tcp any host 100.10.20.45 eq 25
  - access-list 108 permit tcp any eq 25 host 100.10.20.45 **established**
  - (následovat by měla pravidla zpřístupňující DNS serverům)

ACL – příklad 5+6

- Zabraňte úniku paketů z privátní sítě 192.168.0.0/16

- Zabraňte podvržení paketů privátní sítě 192.168.0.0/16 z vnějšku (anti-spoofing filtr)

ACL – příklad 5+6

- Zabraňte úniku paketů z privátní sítě 192.168.0.0/16
  - (Jen) odchozí směr
    - **access-list 109 deny ip 192.168.0.0 0.0.255.255 any**
    - access-list 109 permit ip any any
- Zabraňte podvržení paketů privátní sítě 192.168.0.0/16 z vnějšku (anti-spoofing filtr)
  - (Jen) příchozí směr
    - **access-list 110 deny ip 192.168.0.0 0.0.255.255 any**
    - access-list 110 permit ip any any